Phisher greifen Login-Daten über Microsoft Forms ab - Betrüger zielen auf Active-Directory-Passwörter ab

Das CERT von Retarus warnt vor Phishing-Mails, welche die Empfänger auf ein mit Microsoft Forms erstelltes Formular leiten. Dort sollen sie die Login-Daten ihres Accounts preisgeben. Angeblich seien ihre Security-Einstellungen veraltet und müssen erneuert werden.
"Dear User,

You are still using the old mail security settings for m_____.h____@r_____.com,

Please visit the maintenance portal below to Automatically switch to the new mail settings to avoid service interruption and delays in outgoing/incoming mails."

Die in englischer Sprache verfasste Phishing-Mail richtet sich offensichtlich an Unternehmensanwender und fordert den Empfänger auf, in einem Wartungsportal die Einstellungen seines E-Mail-Accounts zu ändern. Der entsprechende Link führt auf ein mit Microsoft Forms erstelltes Formular, in dem man sich mit seiner E-Mail-Adresse und dem zugehörigen Passwort anmelden soll. "Mit diesem Passwort geben Anwender nicht nur den Zugang zu ihren E-Mails preis", betont Martin Mathlouthi, Product Line Manager Secure Email Platform bei Retarus. "Da Single Sign on üblich ist, handelt es sich gleichzeitig um das Kennwort zum Active Directory und kann den Phishern den Zugang zu weiteren Unternehmensdaten eröffnen."

Empfänger, die E-Mails vom "IT Support" erhalten, sollten genau hinsehen, rät Martin Mathlouthi. Im Unterschied zu anderen Phishing-Mails ist der Text weitgehend fehlerfrei verfasst, nur ein Wort ist falsch geschrieben. Jedoch steht im Absender zwar "IT Support", die hinterlegte E-Mail-Adresse gehört aber nicht zum eigenen Unternehmen oder einem eventuell beschäftigten Support-Dienstleister. Auch im hinterlegten Formular finden sich Hinweise auf den Betrugsversuch. Offenbar um die Microsoft-eigenen Sicherheitsmechanismen zu umgehen, besteht das Wort "Passwort" teilweise aus Sonderzeichen.